Protogate Freeway® Software Requirements Specification (SRS)

DC 900-2021A

Protogate, Inc.

12225 World Trade Drive
Suite R
San Diego, CA
92128
USA
Web: www.protogate.com
Email: sales@protogate.com
Voice: (858) 451-0865
Fax: (877) 473-0190

Protogate Freeway® Software Requirements Specification (SRS): DC 900-2021A

by Protogate, Inc.

Published October 2013

Copyright © 2013 Protogate, Inc.

This Software Requirements Specification (SRS) identifies the requirements which must be satisfied by the Protogate Freeway® software.

The latest version of this document is always available, in a variety of formats and compression options, from the Protogate World Wide Web server (http://www.protogate.com/support/manuals).

This document can change without notice. Protogate, Inc. accepts no liability for any errors this document might contain.

Freeway is a registered trademark of Protogate, Inc. All other trademarks and trade names are the properties of their respective holders.

Table of Contents

Preface ..... **vi**
Purpose of Document vi
Intended Audience vi
Organization of Document vi
Protogate References vi
Document Conventions ix
Revision History ix
Customer Support ix
1. Scope **10**
1.1. Identification 10
1.2. System Overview 10
1.3. Document Overview 10
2. Reference Documents **11**
3. Requirements **12**
3.1. Required States and Modes 12
3.2. Freeway Capability Requirements 12
3.2.1. DLI/TSI Server Requirement 12
3.2.2. ICP Hosting Requirement 12
3.2.3. User Interface Requirements 12
3.3. Freeway External Interface Requirements 12
3.4. Freeway Internal Interface Requirements 12
3.5. Freeway Internal Data Requirements 13
3.6. Adaptation Requirements 13
3.7. Safety Requirements 13
3.8. Security and Privacy Requirements 13
3.8.1. GEN000100 - Supported Release 13
3.8.2. GEN000120 - Supported Components 14
3.8.3. GEN000240 - Network Time-Server 14
3.8.4. GEN000400 - Logon Warning Banner Display 14
3.8.5. GEN000440 - Logging Login Attempts 15
3.8.6. GEN000560 - Password Protect Enabled Accounts 15
3.8.7. GEN001060 - Log Root Access Attempts 15
3.8.8. GEN001100 - Encrypting Root Access 15
3.8.9. GEN001120 - Direct Root Access 16
3.8.10. GEN001640 - Run Control Scripts World Writable Programs or Scripts 16
3.8.11. GEN002040 - Access Control Files Documentation 16
3.8.12. GEN002680 - Audit Logs Accessibility 16
3.8.13. GEN002700 - Audit Logs Permissions 16
3.8.14. GEN002720 - Audit Failed File and Program Access Attempts 17
3.8.15. GEN002740 - Audit File and Program Deletion 17
3.8.16. GEN002760 - Audit Administrative, Privileged, and Security Actions 17
3.8.17. GEN002800 - Audit Login, Logout, and Session Initiation 17
3.8.18. GEN002820 - Audit Discretionary Access Control Permission Modifications 18
3.8.19. GEN002860 - Audit Logs Rotation 18

3.8.20. GEN003820 - Remote Login or Shell is Enabled 18
3.8.21. GEN003840 - The rexec Service is Enabled 18
3.8.22. GEN004220 - The root Account's Browser 18
3.8.23. GEN004400 - File Executed Through Aliases Accessibility 19
3.8.24. GEN004580 - .forward Files 19
3.8.25. GEN004600 - Sendmail Version 19
3.8.26. GEN004620 - Sendmail DEBUG Command 19
3.8.27. GEN004640 - Sendmail DECODE Command 20
3.8.28. GEN005000 - Anonymous FTP Account Shell 20
3.8.29. GEN005020 - Anonymous FTP Configuration 20
3.8.30. GEN005080 - TFTP Secure Mode 20
3.8.31. GEN005100 - TFTP SUID/SGID Bit 20
3.8.32. GEN005140 - TFTP Documentation 21
3.8.33. GEN005200 - X Displays Exporting 21
3.8.34. GEN005300 - Changed SNMP Community Strings 21
3.8.35. GEN005500 - SSH Version 1 Compatibility 21
3.8.36. GEN006380 - NIS/NIS+ Implemented Under UDP 21
3.9. Environment Requirements 22
3.10. Computer Resource Requirements 22
3.10.1. Computer Hardware Requirements 22
3.10.2. Computer Software Requirements 22
3.10.3. Computer Communications Requirements 22
3.11. Software Quality Factors 22
3.12. Design and Implementation Constraints 23
3.13. Personnel-related Requirements 23
3.14. Training-related Requirements 23
3.15. Logistics-related Requirements 23
3.16. Other Requirements 23
3.17. Packaging Requirements 23
3.18. Precedence and Criticality of Requirements 24
4. Qualification Provisions 25
5. Requirements Traceability 31
6. Notes 32
Index 33
Colophon 35

List of Tables

1. Revision History ix
2-1. Referenced Documents 11
4-1. Freeway Software Qualification Methods 25
6-1. Acronym definitions 32

Preface

Purpose of Document

This Software Requirements Specification (SRS) identifies the requirements of the Protogate Freeway® software.

Intended Audience

This document should be read by anyone who needs requirements information about the Protogate Freeway software.

Organization of Document

This document is organized into the following major sections:

Chapter 1

is an overview of this document and of the Protogate Freeway software.

Chapter 2

is a list of other documents referenced by this document.

Chapter 3

describes the Freeway software requirements.

Chapter 4

describes the methods which will be used to ensure that the Freeway software requirements are met.

Chapter 5

traces each software requirement in Chapter 3 to the Freeway software component which satisfies that requirement.

Chapter 6

includes general information to aid in understanding this document.

Protogate References

The following general product documentation list is provided to familiarize you with the available Protogate Freeway and embedded ICP products. Most of these documents are available on-line at Protogate's website

(http://www.protogate.com/). Additional information about documents which are specifically referenced by this Software Requirements Specification (SRS) are in Chapter 2 of this document.

General Product Overview Documents

Freeway 1100 Technical Overview	25-000-0419
Freeway 2000/4000/8800 Technical Overview	25-000-0374
ICP2432 Technical Overview	25-000-0420
ICP6000X Technical Overview	25-000-0522

Hardware Support Documents

Freeway 500 Hardware Installation Guide	DC-900-2000
Freeway 1100/1150 Hardware Installation Guide	DC-900-1370
Freeway 1200/1300 Hardware Installation Guide	DC-900-1537
Freeway 2000/4000 Hardware Installation Guide	DC-900-1331
Freeway 8800 Hardware Installation Guide	DC-900-1553
Freeway 3100 Hardware Installation Guide	DC-900-2002
Freeway 3200 Hardware Installation Guide	DC-900-2003
Freeway 3400 Hardware Installation Guide	DC-900-2004
Freeway 3600 Hardware Installation Guide	DC-900-2005
Freeway 3110 Hardware Installation Guide	DC-900-2012
Freeway 3210 Hardware Installation Guide	DC-900-2013
Freeway 3410 Hardware Installation Guide	DC-900-2014
Freeway 3610 Hardware Installation Guide	DC-900-2015
Freeway 3112 Hardware Installation Guide	DC-900-2016
Freeway 3212 Hardware Installation Guide	DC-900-2017
Freeway 3412 Hardware Installation Guide	DC-900-2018
Freeway 3612 Hardware Installation Guide	DC-900-2019
Freeway ICP6000R/ICP6000X Hardware Description	DC-900-1020
ICP6000(X)/ICP9000(X) Hardware Description and Theory of Operation	DC-900-0408
ICP2424 Hardware Description and Theory of Operation	DC-900-1328
ICP2432 Hardware Description and Theory of Operation	DC-900-1501
ICP2432 Electrical Interfaces (Addendum to DC-900-1501)	DC-900-1566
ICP2432 Hardware Installation Guide	DC-900-1502
ICP2432B Hardware Installation Guide	DC-900-2009

Freeway Software Installation and Configuration Support Documents

Freeway User Guide	DC-900-1333
Freeway Loopback Test Procedures	DC-900-1533

Freeway Release Addendum: Client Platforms	DC-900-1555
Freeway Message Switch User Guide	DC-900-1588
Freeway Software Requirements Specification (SRS)	DC-900-2021
Freeway Ports, Protocols, and Services (PPS)	DC-900-2022
Freeway Software Version Description (SVD)	DC-900-2023
Freeway Lifecycle Support Plan (LSP)	DC-900-2024
Freeway Security Features User's Guide (SFUG)	DC-908-3004
Freeway Security Target (ST)	DC-908-3005

Embedded ICP Software Installation and Programming Support Documents

ICP2432 User Guide for Digital UNIX	DC-900-1513
ICP2432 User Guide for OpenVMS Alpha	DC-900-1511
ICP2432 User Guide for OpenVMS Alpha (DLITE Interface)	DC-900-1516
ICP2432 User Guide for Solaris STREAMS	DC-900-1512
ICP2432 User Guide for Windows NT	DC-900-1510
ICP2432 User Guide for Windows NT (DLITE Interface)	DC-900-1514

Application Program Interface (API) Programming Support Documents

Freeway Data Link Interface Reference Guide	DC-900-1385
Freeway Transport Subsystem Interface Reference Guide	DC-900-1386
QIO/SQIO API Reference Guide	DC-900-1355

Socket Interface Programming Support Documents

Freeway Client-Server Interface Control Document	DC-900-1303

Toolkit Programming Support Documents

Freeway Server-Resident Application (SRA) Programmer Guide	DC-900-1325
OS/Impact Programmer Guide	DC-900-1030
Freeway OS/Protogate Programmer's Guide	DC-900-2008
Protocol Software Toolkit Programmer Guide	DC-900-1338
Protocol Software Toolkit Programmer's Guide (ICP2432B)	DC-900-2007

Protocol Support Documents

ADCCP NRM Programmer Guide	DC-900-1317
Asynchronous Wire Service (AWS) Programmer Guide	DC-900-1324
AUTODIN Programmer Guide	DC-908-1558

Bit-Stream Protocol Programmer Guide	DC-900-1574
BSC Programmer Guide	DC-900-1340
BSCDEMO User Guide	DC-900-1349
BSCTRAN Programmer Guide	DC-900-1406
DDCMP Programmer Guide	DC-900-1343
FMP Programmer Guide	DC-900-1339
Military/Government Protocols Programmer Guide	DC-900-1602
N/SP-STD-1200B Programmer Guide	DC-908-1359
NASCOM Programmer's Guide	DC-900-2010
SIO STD-1300 Programmer Guide	DC-908-1559
TIMI Programmer's Guide	DC-900-2011
X.25 Call Service API Guide	DC-900-1392
X.25/HDLC Configuration Guide	DC-900-1345
X.25 Low-Level Interface	DC-900-1307

Document Conventions

In this document, the term "Freeway" refers to the Freeway software, regardless of which type of Freeway chassis it is running on.

Revision History

The revision history of the Freeway Software Requirements Specification (SRS), Protogate document DC 900-2021, is recorded below:

Table 1. Revision History

Revision	Release Date	Description
DC 900-2021A	October, 2013	Initial Release

Customer Support

If you are having trouble with any Protogate product, call us at 1-858-451-0865 (U.S.) Monday through Friday between 8 a.m. and 5 p.m. Pacific time. You can also fax your questions to us at (858) 451-2865 or (877) 473-0190 any time. Please include a cover sheet addressed to "Customer Service." We are always interested in suggestions for improving our products. You can use the report form in the back of this manual to send us your recommendations.

Chapter 1. Scope

1.1. Identification

This document describes the requirements which must be met by the Protogate Freeway® software, when running on a Protogate Freeway system.

1.2. System Overview

The Protogate Freeway is a data communication system which connects one or more serial-link channels (Wide-Area-Network, or WAN channels) of various types to one or more IP (Internet Protocol) networks. The Freeway acts as a gateway, providing WAN channel access to clients on the IP network.

The Protogate Freeway software is the comprehensive software suite which runs on all Freeways and completely controls them. The Freeway software is based on the FreeBSD operating system, and has been modified to control one or more Protogate Intelligent Communications Processor (ICP) boards. ICP boards are Protogate-manufactured boards which can be installed into a Freeway chassis, plugged into one or more serial-link (WAN) channels, and configured to implement a data communications protocol.

1.3. Document Overview

This document describes the requirements which must be met by the Freeway software. This document is not sensitive or private, and may be disseminated as widely as desired, with no restrictions.

Chapter 2. Reference Documents

A full list of Protogate documents is in the Preface Section of this document.

Documents referenced by this Software Requirements Specification (SRS) are listed in Table 2-1.

Table 2-1. Referenced Documents

Number	Title	Revision	Date
DI-IPSC-81433A	Data Item Description (DID): Software Requirements Specification (SRS)	A	15 Dec, 1999
DC-900-1333	Freeway User's Guide	Q	Sep, 2013
DC-900-1385	Freeway Data Link Interface Reference Guide	E	Mar, 2002
DC-900-1386	Freeway Transport Subsystem Interface Reference Guide	D	Mar, 2002
DC-908-3004	Freeway Security Features User's Guide (SFUG)	A	Oct, 2013

The Protogate documents are available on-line at http://www.protogate.com/support/manuals.

Chapter 3. Requirements

3.1. Required States and Modes

Once booted, a Freeway is always in only one state: ready. All references to any Freeway operation in this document refer to a Freeway in the ready state.

3.2. Freeway Capability Requirements

This section describes the requirements which are specific to the primary mission of most Freeways, which is to enable WAN access via an IP network.

3.2.1. DLI/TSI Server Requirement

The Freeway software must provide a complete DLI/TSI server interface, as described in the two manuals *Freeway Data Link Interface Reference Guide (DC-900-1385)* and *Freeway Transport Subsystem Interface Reference Guide (DC-900-1386)*.

3.2.2. ICP Hosting Requirement

The Freeway software must provide complete support for one or more ICP boards. This support must include not only driver-level support and protocol-downloading support, but also inter-communication between DLI/TSI clients and the ICP board serial data ports.

3.2.3. User Interface Requirements

The Freeway software must provide a user interface to allow one or more users to login and control the operation of the Freeway . Users may login via either an Ethernet interface, or directly through a serial console cable. The user interface must offer the ability for logged-in users to perform all actions which may be necessary to get information about or control the Freeway.

3.3. Freeway External Interface Requirements

The external interfaces of the Freeway software are to one or more DLI/TSI clients (generally across the Ethernet, but may also be via the "localhost" network address from within the Freeway), to one or more data-communications ports (on the ICP boards), and to one or more logged-in users (which may be via a serial console connection, or via an Ethernet connection). The requirements which must be met for each of these interfaces are specified in Section 3.2.

3.4. Freeway Internal Interface Requirements

No internal interface requirements are imposed on the Freeway software; the design of the Freeway software is free to use any internal interfaces which result in meeting the other requirements of this SRS.

3.5. Freeway Internal Data Requirements

No internal data requirements are imposed on the Freeway software; the design of the Freeway software is free to use any internal data structures or designs which result in meeting the other requirements of this SRS.

3.6. Adaptation Requirements

The Freeway will need to be configured to a specific IP address, to allow network clients to connect to it. See the *Freeway User's Guide (DC-900-1333)*. for a description of how to setup and configure a Freeway.

3.7. Safety Requirements

No safety requirements are imposed on the Freeway software.

3.8. Security and Privacy Requirements

The Freeway must be able to be configured to ensure its own security and the security and privacy of all data which passes through it. The specific security and privacy requirements listed here are taken from *UNIX SRG, Version 1, Release 2* published on 02 August, 2012 by the United States Defense Information Systems Agency (DISA). More details about each requirement are in that document, and information about how to verify that a Freeway satisfies each of these requirements is in Chapter 4 of this document, and in Protogate document DC-908-3004: *Freeway Security Features User's Guide (SFUG)*.

The security requirements listed here are not exhaustive; many security features are available on the Freeway which are not included here, either because they are not necessary to the normal operation of a Freeway (for example, participation in the NTP protocol), or because they are so well understood or can be used in so many different ways that listing them here would be confusing (for example, the Freeway firewall). See Protogate document DC-908-3004: *Freeway Security Features User's Guide (SFUG)* for more details about some of those Freeway capabilities.

3.8.1. GEN000100 - Supported Release

Summary	The operating system must be a supported release.

Notes	An operating system release is considered supported if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software.

3.8.2. GEN000120 - Supported Components

Summary	Vendor-recommended software patches and updates, and system security patches and updates, must be installed and up-to-date.
Notes	Timely patching is critical for maintaining the operational availability, confidentiality, and integrity of Information Technology (IT) systems. However, failure to keep operating system and application software patched is a common mistake made by IT professionals. New patches are released daily, and it is often difficult for even experienced system administrators to keep abreast of all the new patches. When new weaknesses in an operating system exist, patches are usually made available by the vendor to resolve the problems. If the most recent recommended updates and security patches are not installed, unauthorized users may take advantage of weaknesses present in the unpatched software. The lack of prompt attention to patching could result in a system compromise.

3.8.3. GEN000240 - Network Time-Server

Summary	The system clock must be synchronized to an authoritative DoD time source.
Notes	To assure the accuracy of the system clock, it must be synchronized with an authoritative time source within DoD. Many system functions, including time-based login and activity restrictions, automated reports, system logs, and audit records depend on an accurate system clock. If there is no confidence in the correctness of the system clock, time-based functions may not operate as intended and records may be of diminished value. Authoritative time sources include authorized time servers within the enclave that synchronize with upstream authoritative sources. Specific requirements for the upstream synchronization of Network Time Protocol (NTP) servers are covered in the Network Other Devices STIG. For systems located on isolated or closed networks, it is not necessary to synchronize with a global authoritative time source. If a global authoritative time source is not available to systems on an isolated network, a local authoritative time source must be established on this network and used by the systems connected to this network. This is necessary to provide the ability to correlate events and allow for the correct operation of time-dependent protocols between systems on the isolated network. If the system is completely isolated (no connections to networks or other systems), time synchronization is not required as no correlation of events between systems will be necessary. If the system is completely isolated, this requirement is not applicable.

3.8.4. GEN000400 - Logon Warning Banner Display

Summary	The Department of Defense (DoD) login banner must be displayed immediately prior to, or as part of, console login prompts.
Notes	Failure to display the login banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.

3.8.5. GEN000440 - Logging Login Attempts

Summary	Successful and unsuccessful logins and logouts must be logged.
Notes	Monitoring and recording successful and unsuccessful logins assists in tracking unauthorized access to the system. Without this logging, the ability to track unauthorized activity to specific user accounts may be diminished.

3.8.6. GEN000560 - Password Protect Enabled Accounts

Summary	The system must not have accounts configured with blank or null passwords.
Notes	If an account is configured for password authentication but does not have an assigned password, it may be possible to log into the account without authentication. If the root user is configured without a password, the entire system may be compromised. For user accounts not using password authentication, the account must be configured with a password lock value instead of a blank or null value.

3.8.7. GEN001060 - Log Root Access Attempts

Summary	The system must log successful and unsuccessful access to the root account.
Notes	If successful and unsuccessful logins and logouts are not monitored or recorded, access attempts cannot be tracked. Without this logging, it may be impossible to track unauthorized access to the system.

3.8.8. GEN001100 - Encrypting Root Access

Summary	Root passwords must never be passed over a network in clear text form.

Notes	If a user accesses the root account (or any account) using an unencrypted connection, the password is passed over the network in clear text form and is subject to interception and misuse. This is true even if recommended procedures are followed by logging on to a named account and using the su command to access root.

3.8.9. GEN001120 - Direct Root Access

Summary	The system must not permit root logins using remote access programs, such as SSH.
Notes	Even though communications are encrypted, an additional layer of security may be gained by extending the policy of not logging directly on as root. In addition, logging in with a user-specific account preserves the audit trail.

3.8.10. GEN001640 - Run Control Scripts World Writable Programs or Scripts

Summary	Run control scripts must not execute world-writable programs or scripts.
Notes	World-writable files could be modified accidentally or maliciously to compromise system integrity.

3.8.11. GEN002040 - Access Control Files Documentation

Summary	There must be no .rhosts, .shosts, hosts.equiv, or shosts.equiv files on the system.
Notes	The .rhosts, .shosts, hosts.equiv, and shosts.equiv files are used to configure host-based authentication for individual users or the system. Host-based authentication is not sufficient for preventing unauthorized access to the system.

3.8.12. GEN002680 - Audit Logs Accessibility

Summary	System audit logs must be owned by root.
Notes	Failure to give ownership of system audit log files to root provides the designated owner and unauthorized users with the potential to access sensitive information.

3.8.13. GEN002700 - Audit Logs Permissions

Summary	System audit logs must have mode 0640 or less permissive.
Notes	If a user can write to the audit logs, audit trails can be modified or destroyed and system intrusion may not be detected. System audit logs are those files generated from the audit system and do not include activity, error, or other log files created by application software.

3.8.14. GEN002720 - Audit Failed File and Program Access Attempts

Summary	The audit system must be configured to audit failed attempts to access files and programs.
Notes	If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

3.8.15. GEN002740 - Audit File and Program Deletion

Summary	The audit system must be configured to audit file deletions.
Notes	If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

3.8.16. GEN002760 - Audit Administrative, Privileged, and Security Actions

Summary	The audit system must be configured to audit all administrative, privileged, and security actions.
Notes	If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

3.8.17. GEN002800 - Audit Login, Logout, and Session Initiation

Summary	The audit system must be configured to audit login, logout, and session initiation.

Notes	If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

3.8.18. GEN002820 - Audit Discretionary Access Control Permission Modifications

Summary	The audit system must be configured to audit all discretionary access control permission modifications.
Notes	If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

3.8.19. GEN002860 - Audit Logs Rotation

Summary	Audit logs must be rotated daily.
Notes	Rotate audit logs daily to preserve audit file system space and to conform to the DoD/DISA requirement. If it is not rotated daily and moved to another location, then there is more of a chance for the compromise of audit data by malicious users.

3.8.20. GEN003820 - Remote Login or Shell is Enabled

Summary	The rsh daemon must not be running.
Notes	The rshd process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.

3.8.21. GEN003840 - The rexec Service is Enabled

Summary	The rexec daemon must not be running.
Notes	The rexecd process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.

3.8.22. GEN004220 - The root Account's Browser

Summary	Administrative accounts must not run a web browser, except as needed for local service administration.
Notes	If a web browser flaw is exploited while running as a privileged user, the entire system could be compromised. Specific exceptions for local service administration should be documented in site-defined policy. These exceptions may include HTTP(S)-based tools used for the administration of the local system, services, or attached devices. Examples of possible exceptions are HP's System Management Homepage (SMH), the CUPS administrative interface, and Sun's StorageTek Common Array Manager (CAM) when these services are running on the local system.

3.8.23. GEN004400 - File Executed Through Aliases Accessibility

Summary	Files executed through a mail aliases file must be owned by root and must reside within a directory owned and writable only by root.
Notes	If a file executed through a mail aliases file is not owned and writable only by root, it may be subject to unauthorized modification. Unauthorized modification of files executed through aliases may allow unauthorized users to attain root privileges.

3.8.24. GEN004580 - .forward Files

Summary	The system must not use .forward files.
Notes	The .forward file allows users to automatically forward mail to another system. Use of .forward files could allow the unauthorized forwarding of mail and could potentially create mail loops which could degrade system performance.

3.8.25. GEN004600 - Sendmail Version

Summary	The SMTP service must be an up-to-date version.
Notes	The SMTP service version on the system must be current to avoid exposing vulnerabilities present in unpatched versions.

3.8.26. GEN004620 - Sendmail DEBUG Command

Summary	The Sendmail server must have the debug feature disabled.

Notes	Debug mode is a feature present in older versions of Sendmail which, if not disabled, may allow an attacker to gain access to a system through the Sendmail service.

3.8.27. GEN004640 - Sendmail DECODE Command

Summary	The SMTP service must not have a uudecode alias active.
Notes	A common configuration for older Mail Transfer Agents (MTAs) includes an alias for the decode user. All mail sent to this user is sent to the uudecode program, which automatically converts and stores files. By sending mail to decode or uudecode aliases present on some systems, a remote attacker may be able to create or overwrite files on the remote host. This could possibly be used to gain remote access.

3.8.28. GEN005000 - Anonymous FTP Account Shell

Summary	Anonymous FTP accounts must not have a functional shell.
Notes	If an anonymous FTP account has been configured to use a functional shell, attackers could gain access to the shell if the account is compromised.

3.8.29. GEN005020 - Anonymous FTP Configuration

Summary	The anonymous FTP account must be configured to use chroot or a similarly isolated environment.
Notes	If an anonymous FTP account does not use a chroot or similarly isolated environment, the system may be more vulnerable to exploits against the FTP service. Such exploits could allow an attacker to gain shell access to the system and view, edit, or remove sensitive files.

3.8.30. GEN005080 - TFTP Secure Mode

Summary	The TFTP daemon must operate in "secure mode" which provides access only to a single directory on the host file system.
Notes	Secure mode limits TFTP requests to a specific directory. If TFTP is not running in secure mode, it may be able to write to any file or directory and may seriously impair system integrity, confidentiality, and availability.

3.8.31. GEN005100 - TFTP SUID/SGID Bit

Summary	The TFTP daemon must have mode 0755 or less permissions.
Notes	If TFTP runs with the setuid or setgid bit set, it may be able to write to any file or directory and may seriously impair system integrity, confidentiality, and availability.

3.8.32. GEN005140 - TFTP Documentation

Summary	Any active TFTP daemon must be authorized and approved in the system accreditation package.
Notes	TFTP is a file transfer protocol often used by embedded systems to obtain configuration data or software. The service is unencrypted and does not require authentication of requests. Data available using this service may be subject to unauthorized access or interception.

3.8.33. GEN005200 - X Displays Exporting

Summary	X displays must not be exported to the world.
Notes	Open X displays allow an attacker to capture keystrokes and to execute commands remotely. Many users have their X Server set to xhost +, permitting access to the X Server by anyone, from anywhere.

3.8.34. GEN005300 - Changed SNMP Community Strings

Summary	SNMP communities, users, and passphrases must be changed from the default.
Notes	Whether active or not, default SNMP passwords, users, and passphrases must be changed to maintain security. If the service is running with the default authenticators, then anyone can gather data about the system and the network and use the information to potentially compromise the integrity of the system or network(s).

3.8.35. GEN005500 - SSH Version 1 Compatibility

Summary	The SSH daemon must be configured to only use the SSHv2 protocol.
Notes	SSHv1 is not a DoD-approved protocol and has many well-known vulnerability exploits. Exploits of the SSH daemon could provide immediate root access to the system.

3.8.36. GEN006380 - NIS/NIS+ Implemented Under UDP

Summary	The system must not use UDP for NIS/NIS+.
Notes	Implementing NIS or NIS+ under UDP may make the system more susceptible to a Denial of Service attack and does not provide the same quality of service as TCP.

3.9. Environment Requirements

The Freeway software is intended to be installed and run only on a Protogate Freeway system. See any of the *Freeway 3xxx Hardware Installation Guide* documents for details about a specific Freeway model -- for example, *Freeway 3412 Hardware Installation Guide (DC-900-2018)*. The Freeway software does not have any other environmental requirements -- though the Freeway is usually connected to an IP network and to one or more serial-link WAN connections, the Freeway software must be able to run without any connections.

3.10. Computer Resource Requirements

This section describes the Freeway's computer resource requirements. The Freeway software always runs on a Protogate Freeway chassis, so it must never require more resources than any Freeway chassis can provide.

3.10.1. Computer Hardware Requirements

The Freeway software is intended to be installed and run only on a Protogate Freeway system. See any of the *Freeway Hardware Installation Guide* documents for details about a specific Freeway model -- for example, *Freeway 3412 Hardware Installation Guide (DC-900-2018)*.

3.10.2. Computer Software Requirements

The Freeway software does not use or require any other software; it is completely self-contained and complete.

3.10.3. Computer Communications Requirements

Depending on the intended use, a Freeway may be connected to one or more serial-link data communication connections, one or more 10baseT/UTP, 100baseTX, 1000baseSx, or 1000baseTx Ethernet IP network connections, and/or a serial link console terminal. However, none of these connections is required, and a Freeway could be configured in such a way that none of these connections is used or necessary.

3.11. Software Quality Factors

The two software quality factors imposed on the Freeway software are that it must maintain high performance and it must be reliable.

As a performance measurement example, when run on any Freeway with 16 8-port ICP boards installed, the Freeway software should be able to send and receive a constant stream of 1000-byte data messages continually and simultaneously on all 128 separate data links, all running at 9600 bits per second -- while simultaneously passing all data messages to and from 128 separate client connections. The Freeway software should be able to perform all that message handling without ever failing to transmit a data message, without losing a data message or any bytes of any data message, without ever reporting the receipt of any data message out of order, and without delaying the transmission or reported reception of any data message.

As a measure of reliability, the Freeway software must be able to perform the performance test described above flawlessly for 7 continuous 24-hour days.

3.12. Design and Implementation Constraints

No design or implementation constraints are imposed on the Freeway software; the design of the Freeway software is free to use any methods or techniques which result in meeting the other requirements of this SRS.

3.13. Personnel-related Requirements

No personnel-related requirements are imposed on the Freeway software.

3.14. Training-related Requirements

No training-related requirements are imposed on the Freeway software.

3.15. Logistics-related Requirements

No logistics-related requirements are imposed on the Freeway software.

3.16. Other Requirements

No other requirements are imposed on the Freeway software.

3.17. Packaging Requirements

No packaging requirements are imposed on the Freeway software.

3.18. Precedence and Criticality of Requirements

All requirements specified in this SRS have equal weight.

Chapter 4. Qualification Provisions

This section defines a set of qualification methods and specifies, for each requirement in Chapter 3, methods or procedures which can be used to ensure that the requirement has been met.

Table 4-1. Freeway Software Qualification Methods

Section	Requirement Name	Qualification Method	Notes
Section 3.2.1	DLI/TSI Server	Test	Setup a Freeway with at least 2 serial datalink ports, loaded with `sps_2432b.mem`, and with a loopback connector between the 2 serial datalink ports; run the spsalp loopback test.
Section 3.2.2	ICP Host	Test	Setup a Freeway with at least 2 serial datalink ports, loaded with `sps_2432b.mem`, and with a loopback connector between the 2 serial datalink ports; run the spsalp loopback test.
Section 3.2.3	User Interface	Test	Login to a Freeway and traverse the user menus.
Section 3.8.1	GEN000100 - Supported Release	Test	Login to a Freeway and execute the command `uname -a`, and verify that the results match the version number listed in the *Freeway Software Version Description (SVD) - DC-900-2023* document.
Section 3.8.2	GEN000120 - Supported Components	Test	Login to a Freeway and execute the command `pkg_info`, and verify that the results match the version numbers listed in the *Freeway Software Version Description (SVD) - DC-900-2023* document.
Section 3.8.3	GEN000240 - Network Time-Server	Check	Login to the Freeway and execute the command `ps -ax |grep "ntpd"` to verify that the ntpd daemon is running, and the command `more /tmp/ntp.conf` to verify that NTP configuration is as desired. If the Freeway has had time to synchronize with other NTP servers, the command `ntpq -p` will show which peers it has synchronized with. See the *Freeway Security Features User's Guide (SFUG) - DC-908-3004* document for details about NTP.
Section 3.8.4	GEN000400 - Logon Warning Banner Display	Check	Login to the Freeway and execute the command `more /etc/ssh/sshd_config` to verify that the "Banner" keyword is set to "`/etc/motd`", and the command `more /etc/motd` to see the text which is displayed upon login. See the *Freeway Security Features User's Guide (SFUG) - DC-908-3004* document for details about the login banner.
Section 3.8.5	GEN000440 - Logging Login Attempts	Check	Login to the Freeway and execute the command `last; grep "authentication error" /var/log/all.log` to verify that both successful and unsuccessful logins are logged. See the *Freeway Security Features User's Guide (SFUG) - DC-908-3004* document for details about logging.

Section	Requirement Name	Qualification Method	Notes
Section 3.8.6	GEN000560 - Password Protect Enabled Accounts	Check	Login to the Freeway, `su - shell` to become a root-level user, and execute the command `awk -F':' '{ if ( $2 == NULL ) print $0; }' < /etc/master.passwd` to verify that there are no users with empty passwords. See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about user accounts.
Section 3.8.7	GEN001060 - Log Root Access Attempts	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `tail -f /var/log/all.log`, then on another login shell execute the command `su - shell`, and verify that a log entry for that appears in the file being displayed in the first shell. See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about user accounts.
Section 3.8.8	GEN001100 - Encrypting Root Access	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `last | grep "^\(root|shell\)" | egrep -v "ttyu" | more;` to verify that root has not logged in over the network, and then the command `ps -axww |grep sshd` to verify that the `sshd` daemon is running. See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about user accounts.
Section 3.8.9	GEN001120 - Direct Root Access	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `find / -name sshd_config -print ; grep -v "^#" /tmp/etc/ssh/sshd_config |grep -i permitrootlogin` to verify that there is no "permitrootlogin yes" line, and therefore that root is not permitted to login directly across the network. See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about user accounts.
Section 3.8.10	GEN001640 - Run Control Scripts World Writable Programs or Scripts	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `ls -l /tmp/boot/rc* ; ls -l /tmp/*sh`, to verify that none are world- or other- writeable. See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about user accounts.
Section 3.8.11	GEN002040 - Access Control Files Documentation	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `find / -name .rhosts ; find / -name .shosts ; find / -name hosts.equiv ; find / -name shosts.equiv`, to verify that none of those files exist. See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about user accounts.

Section	Requirement Name	Qualification Method	Notes
Section 3.8.12	GEN002680 - Audit Logs Accessibility	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `ls -la /var/audit/`, to verify that none of the files in that directory are accessible in any way by any user other than a root-level user (root or shell). See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about file access permissions.
Section 3.8.13	GEN002700 - Audit Logs Permissions	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `more /etc/security/audit_control ; ls -la /var/audit`, to verify that the auditing capability is configured as desired, and that none of the files in `/var/audit/` are accessible in any way by any user other than a root-level user (root or shell). See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about file access permissions.
Section 3.8.14	GEN002720 - Audit Failed File and Program Access Attempts	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `more /etc/security/audit_user`, to verify that "fr" or "-fr" is listed before the second ":" for all users other than the root or shell user. See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about the Freeway auditing.
Section 3.8.15	GEN002740 - Audit File and Program Deletion	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `more /etc/security/audit_user`, to verify that "fd" or "+fd" and "-fd" are listed before the second ":" for all users other than the root or shell user. See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about the Freeway auditing.
Section 3.8.16	GEN002760 - Audit Administrative, Privileged, and Security Actions	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `grep flags /etc/security/audit_control` and `more /etc/security/audit_user`, to verify that either 'ad' or '+ad' and '-ad' are listed on the "flags" line of `/etc/security/audit_control` or before the second ":" for all users other than the root or shell user, in `/etc/security/audit_user`. See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about the Freeway auditing.

Section	Requirement Name	Qualification Method	Notes
Section 3.8.17	GEN002800 - Audit Login, Logout, and Session Initiation	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `grep flags /etc/security/audit_control` to verify that either 'lo' or '+lo' and '-lo' are listed on the "flags" and "naflags" lines of `/etc/security/audit_control`. See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about the Freeway auditing.
Section 3.8.18	GEN002820 - Audit Discretionary Access Control Permission Modifications	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `grep flags /etc/security/audit_control` and `more /etc/security/audit_user`, to verify that either 'fm' or '+fm' and '-fm' are listed on the "flags" line of `/etc/security/audit_control` or before the second ":" for all users other than the root or shell user, in `/etc/security/audit_user`. See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about the Freeway auditing.
Section 3.8.19	GEN002860 - Audit Logs Rotation	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `cat /etc/crontab` and `cat /etc/security/audit_warn`, to find scripts or "`closefile`" commands which rotate audit log files to long-term storage. See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about the Freeway auditing.
Section 3.8.20	GEN003820 - Remote Login or Shell is Enabled	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `grep -v "^#" /etc/inetd.conf |grep rlogind ; grep -v "^#" /etc/inetd.conf |grep rshd` to find any lines which enable the `rlogind` or `rshd` daemons, to verify that neither `rlogind` nor `rshd` are enabled. See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about telnet and rlogin access to a Freeway.
Section 3.8.21	GEN003840 - rexec Service is Enabled	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `grep -v "^#" /etc/inetd.conf |grep rexec` to find any lines which enable the `rexec` daemon, to verify that `rexec` is not enabled. See the *Freeway User's Guide - DC-900-1333* and *Freeway Security Features User's Guide (SFUG) - DC-908-3004* documents for details about telnet and rlogin access to a Freeway.
Section 3.8.22	GEN004220 - Root Account's Browser	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `ls -la /root`, to find any browser configuration files for the root user, to verify that none exist.

Section	Requirement Name	Qualification Method	Notes
Section 3.8.23	GEN004400 - File Executed Through Aliases Accessibility	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `find / -name aliases -depth -print`, to find any "`aliases`" file. That file should not exist anywhere on a Freeway, because Freeways do not support email of any kind.
Section 3.8.24	GEN004580 - .forward Files	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `find / -name .forward -depth -print`, to find any "`.forward`" files. That file should not exist anywhere on a Freeway, because Freeways do not support email of any kind.
Section 3.8.25	GEN004600 - Sendmail Version	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `ls -l /var/mail /etc/mail`, to verify that those directories do not exist, and that sendmail cannot run on the Freeway. Freeways do not support email of any kind.
Section 3.8.26	GEN004620 - Sendmail DEBUG Command	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `telnet localhost 25`, to verify that the result is "Connection refused", because sendmail is not running on the Freeway. Freeways do not support email of any kind.
Section 3.8.27	GEN004640 - Sendmail DECODE Command	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `telnet localhost 25`, to verify that the result is "Connection refused", because sendmail is not running on the Freeway. Freeways do not support email of any kind.
Section 3.8.28	GEN005000 - Anonymous FTP Account Shell	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `grep "^ftp" /etc/passwd`, to verify that there is no active ftp line in `/etc/passwd`, which means that anonymous FTP is not allowed.
Section 3.8.29	GEN005020 - Anonymous FTP Account Shell	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `grep "^ftp" /etc/passwd`, to verify that there is no active ftp line in `/etc/passwd`, which means that anonymous FTP is not allowed.
Section 3.8.30	GEN005080 - TFTP Secure Mode	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `grep "tftp" /etc/inetd.conf`, to verify that tftp is not configured or enabled.
Section 3.8.31	GEN005100 - TFTP SUID/SGID Bit	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `find / -name "*tftpd" -print ; ls -la /usr/libexec/tftpd`, to verify that neither the SUID nor SGID bits are set on the `tftp` file (you should see permission bits similar to "-r-xr-xr-x", with no ’s’ characters).
Section 3.8.32	GEN005140 - TFTP Documentation	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `grep -v "^#" /etc/inetd.conf |grep tftp`, to verify that tftp is not configured or enabled.

Section	Requirement Name	Qualification Method	Notes
Section 3.8.33	GEN005200 - X Displays Exporting	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `ps -ax |grep X`, to verify that Freeway does not run XWindow.
Section 3.8.34	GEN005300 - Changed SNMP Community Strings	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `find / -name snmpd.conf -print ; more /usr/local/share/snmp/snmpd.conf` and look for the "rocommunity" line to verify that it is set to the desired character string.
Section 3.8.35	GEN005500 - SSH Version 1 Compatibility	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `grep -i Protocol 'find / -name sshd_config'` and verify that there is no uncommented line enabling SSH version 1.
Section 3.8.36	GEN006380 - NIS/NIS+ Implemented Under UDP	Check	Login to the Freeway, `su - shell` to become a root-level user, then execute the command `rpcinfo -p | grep yp | grep udp` and verify that it produces an error message, because neither NIS/NIS+ nor rpcbind are running on the Freeway.
Section 3.11	Software Quality	Test	Setup Freeway with a full set of serial datalink ports, loaded with `sps_2432b.mem`, and with loopback connectors between all port pairs; run all possible spsalp loopback tests simultaneously at 9600bps on all the port pairs, for 7 days. While those tests are running, make a separate login to the Freeway and run the `top` utility to verify that "% idle" time is more than 0%.

Chapter 5. Requirements Traceability

This document specifies the software requirements of the Freeway software only, without reference to any higher-level or lower-level components of any other system(s) of which the Freeway software might be a part. There is therefore no traceability of the requirements specified in this SRS to any other system or subsystem requirements.

Chapter 6. Notes

This chapter contains general information to aid in understanding this document.

Table 6-1. Acronym definitions

Acronym	Definition
CSCI	Computer System Configuration Item
DID	Data Item Description
DLI	Data Link Interface
ICP	Intelligent Communication Processor
IP	Internet Protocol
SRS	Software Requirements Specification
TSI	Transport Subsystem Interface
WAN	Wide Area Network

Index

A

Acronyms, 32
  DID (Data Item Description)
    (see DID)
  DISA (Defense Information Systems Agency)
    (see DISA)
  DLI (Data Link Interface)
    (see DLI)
  ICP (Intelligent Communications Processor)
    (see ICP)
  IP (Internet Protocol)
    (see IP)
  SRG (Security Requirements Guide)
    (see SRG)
  SRS (Software Requirements Specification)
    (see SRS)
  STIG (Security Technical Implementation Guide)
    (see STIG)
  TSI (Transport Subsystem Interface)
    (see TSI)
  WAN (Wide Area Network)
    (see WAN)
Adaptation Requirements, 13
Audience, vi

C

Computer Resource Requirements, 22
CSCI, 32
Customer support, ix

D

Data Item Description
  (see DID)
Data Link Interface
  (see DLI)
Defense Information Systems Agency
  (see DISA)
Design and Implementation Constraints, 23
DID, 11, 32
DISA, 13
DLI, 12, 32
Document conventions, ix

E

Environment Requirements, 22

F

Freeway Capability Requirements, 12
Freeway External Interface Requirements, 12
Freeway Internal Data Requirements, 13
Freeway Internal Interface Requirements, 13

I

ICP, 10, 12, 32
Identification, 10
Intelligent Communications Processor
  (see ICP)
Internet Protocol
  (see IP)
IP, 10, 32

L

Logistics-related Requirements, 23

N

Notes, 32

O

Other Requirements, 23

P

Packaging Requirements, 23
Personnel-related Requirements, 23
Precedence and Criticality of Requirements, 24
Preface, vi
Product support, ix

Q

Qualification methods, 25
Qualification Provisions, 25

R

Reference documents, vi, 11
Required States and Modes, 12
Requirements Traceability, 31

S

Safety Requirements, 13
Security and Privacy Requirements, 13
Security Requirements Guide
(see SRG)
Security Technical Implementation Guide
(see STIG)
Software Quality Factors, 23
Software Requirements Specification
(see SRS)
SRG, 13
SRS, 32
STIG, 13
Support, product, ix

T

Technical support, ix
Training-related Requirements, 23
Transport Subsystem Interface
(see TSI)
TSI, 12, 32

W

WAN, 10, 32
Wide Area Network
(see WAN)

Customer Report Form

Customer Report Form

We at Protogate are constantly striving to improve our products. If you have any suggestions or problems you would like to report regarding our hardware, software, or documentation, please complete the following form and mail it to us at Protogate, Inc., 12225 World Trade Drive, Suite R, San Diego, CA, 92128, USA. Or contact us via email: <sales@protogate.com>, voice: (858) 451-0865, or fax: (877) 473-0190. Please also include the document title or number and the section and page number, if applicable.

Your Name and Phone Number:

_____

Company:

_____

Address:

_____

_____

_____

Product:

_____

Problem or Suggestion:

_____

_____

_____

_____

_____

Thank you.